PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2006/07

SAM Moneo : Composant AT90SC12836RCT-E masqué par l'application SAM_MONEO 1.3.0 développée par Sagem (réf. : AT58819E / 1.3.0)

Paris, le 29 mai 2006

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Synthèse

Rapport de certification 2006/07

SAM Moneo : Composant AT90SC12836RCT-E masqué par l'application SAM_MONEO 1.3.0 développée par Sagem (réf. : AT58819E / 1.3.0)

Développeurs : Atmel, Sagem Défense Sécurité

Critères Communs version 2.2

EAL4 Augmenté
(ADV_IMP.2, ALC_DVS.2, AVA_VLA.4)

conforme au profil de protection PP/9911

Commanditaire : BMS

Centre d'évaluation : CEA-LETI

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics. (article 7)
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. (article 8)

Les procédures de certification sont publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

Accords de reconnaissance des certificats

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

La direction centrale de la sécurité des systèmes d'information passe aussi des accords de reconnaissance avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties. (article 9 du décret 2002-535)

Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance mutuelle s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.

[2] En mai 2005, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada, l'Australie-Nouvelle Zélande et le Japon ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède, la Turquie, la République Tchèque, Singapour et l'Inde.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est SAM Moneo : Composant AT90SC12836RCT-E masqué par l'application SAM_MONEO 1.3.0 développée par Sagem Défense Sécurité (réf. : AT58819E / 1.3.0) .

1.2. Développeur

SAGEM Défense Sécurité

Avenue du Gros Chêne
95610 Eragny sur Oise
France

ATMEL

Maxwell Building
Scottish Eterprise Technology Park
Birniehill Roundabout
East Kilbride G75 0QR
Grande-Bretagne

1.3. Description du produit évalué

1.3.1. Architecture

Le produit est un composant masqué (référence : AT58819E / 1.3.0) destiné à être utilisé dans une carte à puce. Il est constitué

- d'un micro-circuit AT90SC12836RCT (référence : AT58819 révision E) développé et fabriqué par ATMEL ;
- d'un logiciel SAM_MONEO 1.3.0 développé par Sagem Défense Sécurité masqué dans la mémoire ROM du micro-circuit .

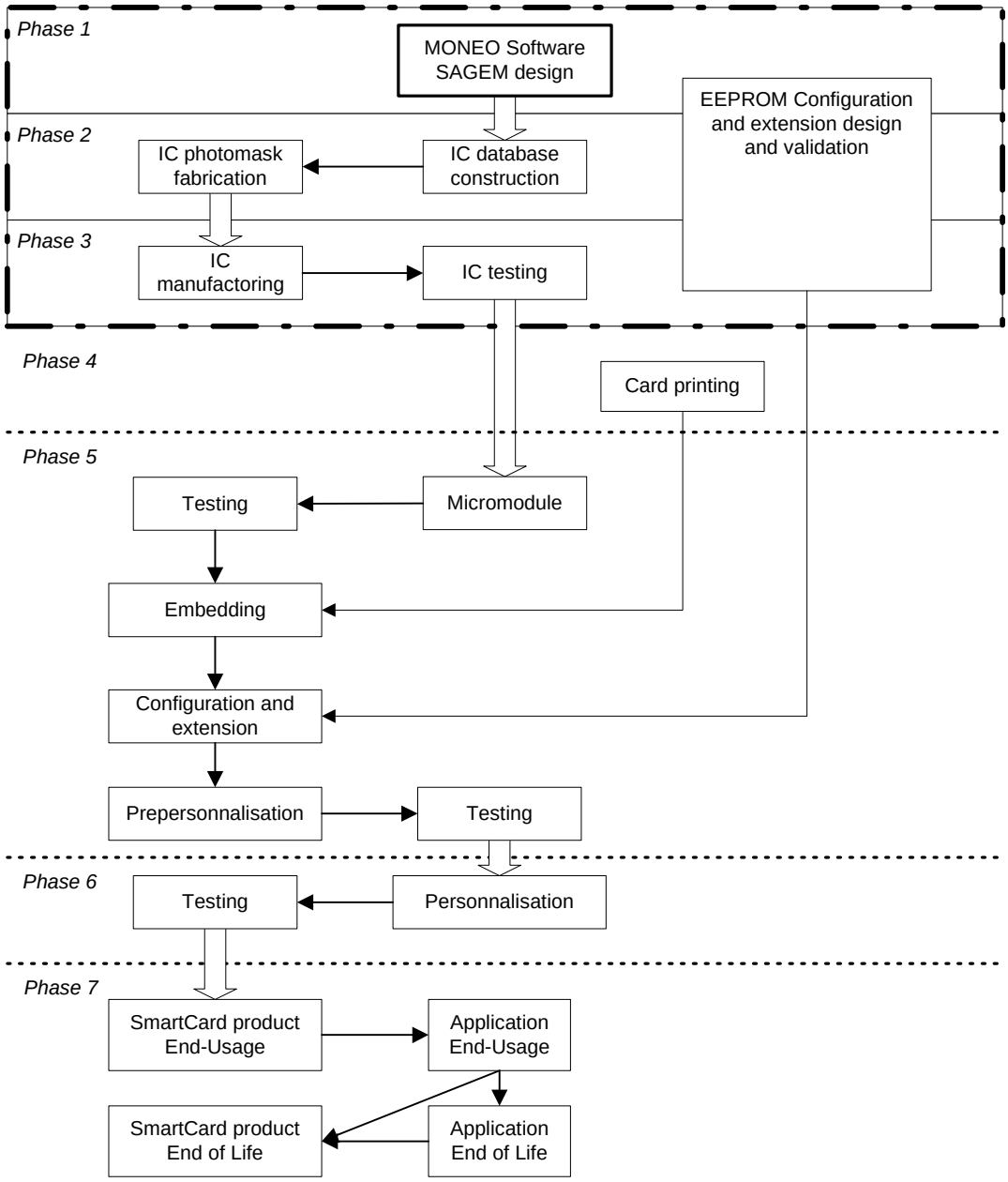
Ce logiciel est composé des modules suivants :

- d'un système d'exploitation ;
- d'une application AIP (fonctions d'initialisation et de personnalisation) ;
- d'une application SAM MONEO.

Le produit ne contient aucun patch. Le produit est disponible sous une seule configuration.

1.3.2. Cycle de vie

Le cycle de vie du produit, qui suit les phases définies dans le profil de protection PP/9911, est le suivant :



1.3.3. Périmètre et limites du produit évalué

Le produit évalué est un module d'accès sécurisé (SAM : Security access module) destiné à être utilisé dans le système de porte-monnaie électronique Moneo. Le SAM est inclus dans un terminal de paiement (PD : Purchase Device) utilisé par un commerçant pour effectuer des transactions de valeur électronique.

Le produit est utilisé pour effectuer trois types de transactions :

- crédit : le terminal de paiement débite de la valeur électronique d'un porte-monnaie électronique (IEP : Intersector Electronic Purse) ;
- chargement rapide : le terminal de paiement crédite de la valeur électronique sur un porte-monnaie électronique ;
- collecte : le terminal de paiement envoie le montant de la valeur électronique collectée à l'émetteur de la valeur électronique via un dispositif d'acquisition.

Les fonctions d'initialisation et de personnalisation (application AIP) de la carte SAM MONEO n'ont pas été évaluées.

2. L'évaluation

2.1. Contexte

L'évaluation a été effectuée selon le schéma de composition défini dans le document [COMP]. La composition consiste à réaliser l'évaluation d'un composant masqué en évaluant d'une part le micro-circuit, et d'autre part le logiciel, en vérifiant qu'aucune faiblesse n'est introduite par l'intégration du logiciel sur le micro-circuit.
Cette évaluation a été réalisée sur la base des résultats de l'évaluation du micro-circuit ATMEL AT90SC12836RCT (Réf. AT58819 Rév. E) au niveau EAL4 augmenté des composants, ADV_IMP.2, AVA_MSU.3 ALC_DVS.2, et AVA_VLA.4, conforme au profil de protection [PP9806]. Ce micro-circuit a été certifié le 9 août 2005 sous la référence 2005/20 [2005/20]. Le niveau de résistance du produit aux attaques a été confirmé le 17 mars 2006 dans le cadre du processus de surveillance.

Le produit évalué est une évolution du produit « Composant AT05SC3208R masqué par l'application SAM Moneo développée par Sagem (référence AT568D6 EB AA) », certifié en 2003 sous la référence 2003/19 [2003/19].
Une partie des verdicts de la présente évaluation s'appuie donc sur les résultats des travaux menés lors cette précédente évaluation.

Cette évaluation bénéficie également de la réutilisation de résultats de travaux réalisés lors d'autres évaluations de masques.

2.2. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM]. Les interprétations 38, 56, 103, 104, 111, 140, 141, 150, 151, 201, 202, 212, 222 ont également été prises en compte.

Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au CESTI, validées par la DCSSI et compatibles avec le document [AIS34] ont été utilisées.

2.3. Commanditaire

BMS

25 rue de Ponthieu
75008 Paris
France

2.4. Centre d'évaluation

CEA - LETI

17 rue des martyrs
38054 Grenoble Cedex 9
France

Téléphone : +33 (0)4 38 78 40 87
Adresse électronique : alain.merle@cea.fr

2.5. Rapport technique d'évaluation

L'évaluation s'est déroulée du 28 novembre 2005 au 5 mai 2006.

Le rapport technique d'évaluation [RTE] détaille les travaux menés par l'évaluateur et présente les résultats obtenus. Les sections suivantes récapitulent les principaux aspects évalués.

2.6. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Cette cible de sécurité est conforme au profil de protection « Micro-circuit pour carte à puce avec un logiciel embarqué », PP/9911 [PP9911]. De plus, cette cible de sécurité est basée sur le PP/0101 [PP0101] pour les exigences concernant le SAM.

Pour les tâches d'évaluation de la cible de sécurité, les verdicts suivants ont été émis par l'évaluateur, ces verdicts s'appuient sur ceux du certificat [2003/19] :

Classe ASE: Evaluation d'une cible de sécurité		**Verdicts**
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite

2.7. Evaluation du produit

2.7.1. Les tâches d'évaluation

Les tâches d'évaluation réalisées correspondent au niveau d'évaluation EAL4[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL4	Methodically designed, tested, and reviewed
+ ADV_IMP.2	Implementation of the TSF
+ ALC_DVS.2	Sufficiency of security measures
+ AVA_VLA.4	Highly resistant

2.7.2. L'évaluation de l'environnement de développement

Le produit est développé sur le site de :

SAGEM Défense Sécurité

Avenue du Gros Chêne
95610 Eragny sur Oise
France

Les mesures de sécurité analysées par l'évaluateur permettent de maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation lors du développement.

L'évaluateur a analysé le plan de gestion de configuration fourni par le développeur qui précise l'utilisation du système de gestion de configuration. Le système permet de générer notamment la liste de configuration [CONF] qui identifie tous les éléments gérés par le système.

Pour les tâches d'évaluation liées à l'environnement de développement, les verdicts suivants ont été émis par l'évaluateur :

Classe ACM: Gestion de configuration		**Verdicts**
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Classe ALC: Support au cycle de vie		**Verdicts**
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	Réussite

2.7.3. L'évaluation de la conception du produit

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles identifiées dans la cible de sécurité et listées ci-après sont correctement et

[1] Annexe 1 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

complètement raffinées dans les niveaux suivants de représentation du produit : spécifications fonctionnelles (FSP), conception de haut-niveau (HLD), conception de bas-niveau (LLD), implémentation (IMP).

Les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :

- Audit data generation (FAU_GEN.1);
- Potential violation analysis (FAU_SAA.1);
- Audit review (FAU_SAR.1);
- Protected audit trail storage (FAU_STG.1);
- Cryptographic key access (FCS_CKM.3);
- Cryptographic key destruction (FCS_CKM.4);
- Cryptographic operation (FCS_COP.1);
- Enforced proof of origin (FCO_NRO.2);
- Enforced proof of receipt (FCO_NRR.2);
- Complete access control (FDP_ACC.2);
- Security attributes based access control (FDP_ACF.1);
- Basic data authentication (FDP_DAU.1);
- Export of user data without security attributes (FDP_ETC.1);
- Subset information flow control (FDP_IFC.1);
- Simple security attributes (FDP_IFF.1);
- Import of user data without security attributes (FDP_ITC.1);
- Subset residual information protection (FDP_RIP.1);
- Stored data integrity monitoring and action (FDP_SDI.1);
- Stored data integrity monitoring and action (FDP_SDI.2);
- Authentication failures handling (FIA_AFL.1);
- User attribute definition (FIA_ATD.1);
- Timing of authentication (FIA_UAU.1);
- Unforgeable authentication (FIA_UAU.3);
- Single-use authentication mechanisms (FIA_UAU.4);
- Re-authenticating (FIA_UAU.6);
- Timing of identification (FIA_UID.1);
- User-subject binding (FIA_USB.1);
- Management of security functions behaviour (FMT_MOF.1);
- Management of security attributes (FMT_MSA.1);
- Secure security attributes (FMT_MSA.2);
- Static attribute initialisation (FMT_MSA.3);
- Management of TOE security functions data (FMT_MTD.1);
- Specification of management functions (FMT_SMF.1);
- Security management roles (FMT_SMR.1);
- Unobservability (FPR_UNO.1);
- Failure with preservation of secure state (FPT_FLS.1);
- Notification of physical attack (FPT_PHP.2);
- Resistance to physical attack (FPT_PHP.3);
- Replay detection (FPT_RPL.1);
- Non-bypassability of the TSP (FPT_RVM.1);
- TSF domain separation (FPT_SEP.1);
- Inter-TSF basic TSF data consistency (FPT_TDC.1);
- TSF testing (FPT_TST.1).

Pour les tâches d'évaluation liées à la conception du produit, les verdicts suivants ont été émis par l'évaluateur :

Classe ADV: Développement		**Verdicts**
ADV_SPM.1	Informal TOE security policy model	Réussite
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite

2.7.4. L'évaluation des procédures de livraison et d'installation

L'évaluateur a analysé les procédures de livraison du produit entre Sagem Défense Sécurité et Atmel.
Ces procédures permettent de connaître l'origine de la livraison et de détecter une modification du produit au cours de cette livraison.

L'installation du produit correspond à l'identification du produit avant son utilisation. Les procédures analysées [INSTALL] permettent d'obtenir une configuration sûre de l'application.

Pour les tâches d'évaluation liées aux procédures de livraison et d'installation, les verdicts suivants ont été émis par l'évaluateur :

Classe ADO: Livraison et exploitation		**Verdicts**
ADO_DEL.2	Detection of modification	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite

2.7.5. L'évaluation de la documentation d'exploitation

Pour l'évaluation, les différentes utilisations du produit ont été considérées :

Phase du cycle de vie	**Rôle**	**Utilisation**
4 et 5	Administrateur	Pré-personnalisateur
6	Administrateur	Personnalisateur
7	Administrateur	Autorité de domaine et émetteur
	Administrateur	Émetteur
	Utilisateur	Terminal de paiement du commerçant

L'évaluateur a analysé les guides d'administration et d'utilisation [GUIDES] pour s'assurer qu'ils permettent d'exploiter le produit évalué d'une manière sécurisée.

Pour les tâches d'évaluation liées à la documentation d'exploitation, les verdicts suivants ont été émis par l'évaluateur :

Classe AGD: Guides		**Verdicts**
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite

2.7.6. L'évaluation des tests fonctionnels

L'évaluateur a analysé la documentation des tests réalisés par le développeur pour s'assurer que toutes les fonctionnalités du produit listées dans la cible de sécurité ont bien été testées.

L'évaluateur a également réalisé des tests fonctionnels pour s'assurer, de manière indépendante, du fonctionnement correct du produit évalué.

L'évaluateur a réalisé ses tests fonctionnels indépendants sur des échantillons fournis par le développeur.

Pour les tâches d'évaluation liées aux tests fonctionnels, les verdicts suivants ont été émis par l'évaluateur :

Classe ATE: Tests		**Verdicts**
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite

2.7.7. L'évaluation des vulnérabilités

L'évaluateur s'est assuré que la documentation fournie avec le produit [INSTALL] [GUIDES] est suffisamment claire pour éviter des erreurs d'exploitation qui pourraient mener à un état non sûr du produit.

Les fonctions suivantes (identifiées dans la cible de sécurité ST) :
- PD authentication by the IEP (MONEO_FS1),
- IEP authentication by the PD (MONEO_FS2),
- Access protection to the user data (MONEO_FS7),
- Replay protection (MONEO_FS10),
- PD authentication by the Acquirer (MONEO_FS14),

ont fait l'objet d'une estimation du niveau de résistance intrinsèque. Le niveau de résistance de ces fonctions est jugé élevé : **SOF-high**.

En s'appuyant sur une analyse de vulnérabilités réalisée par le développeur et sur toutes les informations qui lui ont été livrées dans le cadre de l'évaluation, l'évaluateur a réalisé sa propre analyse indépendante pour estimer les vulnérabilités potentielles du produit. Cette analyse a été complétée par des tests sur les échantillons fournis par le développeur.

L'analyse réalisée par l'évaluateur n'a pas permis de démontrer l'existence de vulnérabilités exploitables pour le niveau visé. Le produit peut donc être considéré comme résistant à des attaques de niveau **élevé**.

Pour les tâches d'évaluation liées aux vulnérabilités, les verdicts suivants ont été émis par l'évaluateur :

Classe AVA : Estimation des vulnérabilités		**Verdicts**
AVA_MSU.2	Validation of analysis	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.4	Highly resistant	Réussite

2.7.8. L'analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques n'a pas été analysée par la DCSSI.

3. La certification

3.1. Conclusions

L'ensemble des travaux réalisés par le centre d'évaluation et décrits dans le rapport technique d'évaluation [RTE] permet la délivrance d'un certificat conformément au décret 2002-535.
Ce certificat atteste que l'exemplaire du produit soumis à évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST]. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. (Art. 8 du décret 2002-535)

3.2. Restrictions d'usage

Les conclusions de l'évaluation ne sont valables que pour le produit spécifié au chapitre 1 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation résumés ci-dessous et suivre les recommandations se trouvant dans les guides fournis [INSTALL] [GUIDES] :

- la communication entre la carte porteur et le terminal de paiement doit être sécurisée (en terme de protocole et de procédure) (O.USE_DIAG) ;
- le fournisseur de valeur doit garantir la valeur électronique dans l'ensemble du système. Les acteurs du système (y compris le porteur du porte-monnaie électronique) doivent appliquer la politique de sécurité du système, cette dernière devant être communiquée au porteur du porte-monnaie électronique par le fournisseur de valeur électronique (O.SYSTEM) ;
- les appareils de chargement et d'acquisition ne doivent pas créer de valeur électronique, mais seulement distribuer aux parties autorisées le même montant de valeur électronique qu'ils reçoivent (O.EV_DISTRIB) ;
- les appareils de chargement doivent entrer dans un état sûr suite à une défaillance durant une transaction de chargement ou une transaction anormale ou bien lors du re-jeu d'une transaction, sans perte ou création de valeur électronique (O.LA_FAIL) ;
- l'application de l'appareil de chargement doit s'exécuter dans un domaine logique de sécurité disponible à cet effet, afin de prévenir les interférences et les altérations pouvant être provoquées par des agents frauduleux (O.LA_DOMAIN) ;
- les appareils de chargement doivent enregistrer tous les événements et/ou données nécessaires, contribuant à une gestion efficace du système (O.LA_RECORD) ;
- les appareils de chargement et d'acquisition doivent prévenir les accès et les opérations effectués par les utilisateurs sur des ressources sur lesquelles ils n'ont pas de permissions (O.AUTH2) ;
- durant un chargement, l'appareil de chargement doit maintenir deux domaines de sécurité distincts : le domaine de transaction de débit, et le domaine de transaction de chargement du porte-monnaie électronique (O.PSEUDO) ;
- les fournisseurs de porte-monnaie électronique doivent s'assurer que la cible d'évaluation est délivrée et installée de manière à maintenir le niveau de sécurité (O.INSTALL) ;

- les fournisseurs de porte-monnaie électronique doivent s'assurer que la cible d'évaluation est gérée, administrée de manière à maintenir le niveau de sécurité (O.MANAGE) ;
- les appareils d'acquisition doivent entrer dans un état sûr lors de défaillance lors des transactions, lors d'une transaction anormale ou bien lors du re-jeu d'une transaction, sans perte ou création de valeur électronique (O.ACQ) ;
- les appareils d'acquisition doivent enregistrer tous les événements et/ou données nécessaires, contribuant à une gestion efficace du système (O.A_RECORD) ;
- la carte porteur doit être conforme aux objectifs qui la concernent tels que spécifiés dans le PP/0101 (O.IEP_EVAL) ;
- le montant de valeur électronique stockée dans la carte porteur doit être limité à un seuil maximal (O.LIMIT).

Annexe 1. Niveaux d'assurance prédéfinis EAL

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 2. Références documentaires du produit évalué

[PP9911]	▪ Eurosmart Protection Profile, Smart Card Integrated Circuit With Embedded Software, PP/9911, v2.0, June 1999
[PP0101]	▪ Intersector Electronic Purse and Purchase Device (version without Last Purchase Cancellation) v1.3, March 2001
[2003/19]	▪ Rapport de certification 2003/19 du 04/11/03 Composant AT05SC3208R masqué par l'application SAM Moneo développée par SAGEM (référence AT568D6 EB AA)
[2005/20]	▪ Rapport de certification 2005/20 du 09/08/05 Micro-circuit ATMEL AT90SC12836RCT rev. E
[CONF]	▪ Fiche de Version du Logiciel SAM_MONEO_1_3 Composant ATMEL SK0000034200 v02 du 08/03/06
[GUIDES]	▪ Guide d'utilisation du Key Center (BMS) Réf. :GUI-GDC-001 v1.2 du 24/03/06 ▪ Spécifications d'interface Carte/ Terminal/ Central (BMS) Réf.DSI8 v1.6.2 ▪ MDA (Modification de document applicable) DSI8 (BMS) Réf. : 06100004 ▪ Différentiel fonctionnel SIRIUS Réf. : SK 0000039375 Rév. :1.0 du 09/03/06 ▪ SAM MONEO : Initialization and Personalization Réf. : ERA U32 DR 090 - 03 Rév.:G du 12/01/06
[INSTALL]	▪ SAM MONEO : Initialization and Personalization Réf. : ERA U32 DR 090- 03 Rév.:G du 12/01/06 ▪ Document d'installation, de génération et de démarrage ERA U32 DR 069 - 03 Rév. : D du 19/10/05
[RTE]	▪ Rapport Technique d'évaluation Réf. :LETI.CESTI.SIR.RTE.001 v1.0 du 03/05/06
[ST]	▪ SAM MONEO: SECURITY TARGET Réf. : ERA U32 CIS 06-02 Rév. :J du 27/03/06

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CC IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, version 1.2, July 2000.
[CC AP]	Common Criteria supporting documentation - Application of attack potential to smart-cards, version 1.1, July 2002.
[COMP]	Common Criteria supporting documentation – ETR-lite for composition: Annex A - Composite smartcard evaluation : Recommended best practice, Version 1.2, March 2002.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[AIS34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr